HP Enterprise Services

Service Center User Manual for HIPAA Compliant Electronic Transactions

Nevada Medicaid Management Information System (NV MMIS)

State of Nevada
Department of Health and Human Services (DHHS)
Division of Health Care Financing and Policy (DHCFP)

Version 2.0
December 5, 2011

Change history

Date (mm/dd/yyyy)	Description of changes	Pages impacted
12/05/2011	Takeover HPES	All

Table of contents

Introduction

This manual presents procedures for submitting and retrieving electronic transactions between service centers and HP Enterprise Services (HPES). A service center may be a one-person provider office or a clearinghouse servicing thousands of providers.

Electronic transactions (also known as Electronic Data Interchange or EDI) give Nevada Medicaid providers the capability of accelerated services including:

- ☐ Medicaid claims submission
- ☐ Claims status request and response
- ☐ Eligibility request and response
- ☐ Prior authorization request and response
- ☐ Pharmacy Point-of-Sale transactions
- ☐ Electronic Remittance Advices

Electronic transactions reduce the time for receipt of Medicaid claims to HPES by eliminating the time-consuming process of document preparation, mailing, transaction receipt and data entry. Unlike paper claims, electronic transactions are transmitted directly to HPES and processed the same day.

Contacting the EDI Coordinator

The HPES EDI Coordinator assists providers and Service Centers with EDI enrollment, testing and technical support.

Contact the EDI Coordinator at:

HP Enterprise Services
EDI Coordinator
PO Box 30042
Reno Nevada 89520-3042

Phone: (877) 638-3472
Fax: (775) 784-7932
E-mail: nvmmis.EDIsupport@hp.com

HIPAA Requirements

All electronic transactions must be in the HIPAA specified format.

HIPAA compliant electronic transaction software must be used for electronic transactions between service centers and HPES. Providers may purchase and use this software to submit and retrieve electronic transactions directly from their practice location or contract with a larger service center to submit and receive the electronic transactions on their behalf.

Disclaimer

This document, and all associated materials, was developed as an aid for Nevada Division of Health Care Financing and Policy (DHCFP) Providers to understand the federal obligations imposed by the Health Insurance Portability and Accountability Act (HIPAA) and is for informational use only. Neither HPES nor the State of Nevada can provide any legal advice or statement of law regarding providers' obligations under federal law. HPES and the State of Nevada cannot warranty any information contained herein. As with any matter of law, independent legal counsel should be consulted regarding compliance with HIPAA.

EDI Enrollment

The forms discussed below are on the HPES web site at http://Medicaid.nv.gov.

Electronic transactions may be sent to and retrieved from HPES only after the following enrollment documents have been submitted and successful transaction testing has taken place (see heading, Testing).

Please complete the EDI enrollment forms as described below. If the EDI enrollment forms are not complete when submitted to the EDI Coordinator, a fax will be sent to you describing the missing information.

Electronic Transaction Agreement for Service Centers (FA-35)

Enter the name and address of the service center as requested in the top section of this agreement and the date on which this document was signed. An owner or authorized agent must sign and date this form and provide their professional title in the space provided. Leave blank the fields on the lower right of this form under HPES. These fields will be completed by HPES upon receipt of the agreement.

Service Center Operational Information (FA-36)

Each service center must complete and submit this form to HPES. This form notifies HPES of the service center's contact information, electronic transaction types and software vendor information.

Check the box next to each electronic transaction you wish to provide. Note that you must test each of these transactions prior to being able to submit or retrieve them in production.

Service centers are required to notify HPES of any change to information presented on this form within five business days. When using this form to change service center information, please check the box near the top of the form to indicate that this is a change to previous information on file with HPES.

Service Center Authorization (FA-37)

The service center Authorization (FA-37), notifies HPES that a provider, clearinghouse or intermediary wishes to authorize or terminate electronic transaction services.Providers sending and receiving electronic transactions on their own behalf must complete and submit this form designating their own practice as the

service center.

Providers must submit a Service Center Authorization for each National Provider Identifier (NPI) or Atypical Provider Identifier (API) used when submitting claims to HPES. For example, if a provider has three different NPIs, that provider must submit three Service Center Authorizations.

A provider uses the Service Center Authorization to:

- Authorize transactions with a Service Center ☐
- Terminate transactions with a Service Center ☐
- Authorize a service center to process the provider's Remittance Advice (RA)
- Terminate authorization for a service center to process the provider's RA

Following submission of the appropriate enrollment forms, HPES provides the service center with a service center code. HPES will contact you by phone with your SFTP server username, your service center code and your initial password.

Follow the instructions below to complete the Service Center Authorization Form for Providers.

- Enter the service center name and code in the shaded area at the top of the form.
- If this form is submitted at the same time as FA-35 and FA-36, leave the code field blank. Otherwise this service center code must be entered. This code is available by contacting the service center with whom you have contracted.
- For the first two form items in bold, check the appropriate box(es) to indicate which services you are authorizing or terminating with the service center shown in the shaded area at the top of the form.
- If you do not fill in the Begin Date field, the date on which HPES received the form will be used. If terminating electronic transaction services, the date on which you would like those services to end (Termination Date) must be entered.
- When authorizing a service center to submit or retrieve a transaction on your behalf, please make sure the service center is authorized by HPES to submit that type of transaction. Contact your service center directly to inquire about which electronic transactions they provide.
- The last two form items allow providers to authorize or terminate electronic Remittance Advice (RA) processing with a service center. Although you may authorize multiple service centers to send and retrieve electronic transactions on your behalf, only one service center may process your electronic RA. If you would like an electronic RA, check the appropriate box.
- Please note that 30 days after you are set up to receive electronic RA, all paper RAs to you will cease. If during the first 30 days, you decide that the electronic RA is not working for you, you should fax another Provider Service Center Authorization to the EDI Coordinator placing a check mark in the appropriate box to terminate the electronic RA so your paper remittances will continue.
- Read and understand the last paragraph before signing this form.

Edits

To submit electronic Medicaid transactions, a service center must conform to record formats and specifications as outlined in the Implementation Guides and Nevada Medicaid Companion Guides. These guides are included on the HPES web site at http://medicaid.nv.gov.

All files must pass through Nevada Medicaid's X12 compliance checker to ensure proper format and compatibility. It is to the service center's advantage to ensure that complete and accurate information is entered as required on an entryby-entry basis. Missing or invalid data may cause claims to pend or be denied thereby reducing the benefits of electronic submission.

All electronic claims submitted to HPES must be in the HIPAA compliant format. Currently, this format is ANSI X12N Version 4010A1.
HPES supports the following Transaction Sets:

Transaction 270: Recipient eligibility request to verify Medicaid benefits and coverage
Transaction 271: Recipient eligibility response from the HPES Eligibility Verification System (EVS) providing benefit and coverage information for a Medicaid recipient

Transaction 276: Claim status inquiry to request the status of a claim submitted to HPES

Transaction 277: Response from HPES to report the status of a claim

Transaction 277u: Unsolicited response
Transaction 278: Prior authorization or referral request and response
Transaction 820: Premium payment for enrolled HMO members
Transaction 834: Enrollment/Dis-Enrollment to an HMO
Transaction 835: Electronic Remittance Advice from HPES showing the status and payment amounts of a provider's claims
Transaction 837D: Dental Health Care Claim or Encounter for providers using the ADA dental claim form

Transaction 837I: Institutional Health Care Claim or Encounter for providers using the UB-04 claim form

Transaction 837P: Professional Health Care Claim or Encounter for providers using the CMS-1500 claim form

Transaction NCPDP: National Council for Prescription Drug Programs Batch

HPES certifies its outbound data through Level 6 using the Claredi tool. For providers, we strongly recommended that all software used for electronic Medicaid transactions be pre-tested and certified by an independent certification agent such as Claredi through Level 2 at a minimum. Certification through Level 2 is a requirement for service centers submitting claims for clearinghouses, software vendors and intermediaries.

Secure FTP Guidelines

Each service center is responsible for purchasing or obtaining compatible FTP client software that supports 128-bit Explicit Secure Socket Layer (SSL) file transfer. There are several commercially available client software packages as well as a few software packages that are available through Internet downloads.

HIPAA transactions require that all service centers use FTP server/client software for sending and retrieving electronic data. Service centers must test the use of this software prior to submitting electronic transactions for processing. The FTP client software must comply with Internet standards for the FTP protocol. RFC 2246 and RFC 2228 define the SSL FTP standards and are on the Internet at http://www.ietf.org.

The HPES SFTP server requires an SSL connection from the service center to ensure that user login and data transactions meet HIPAA privacy and security requirements. All files electronically sent to and received from HPES must be in ANSI X12N Version 4010A1 format and must utilize this SSL FTP connection. Both the login to the HPES SFTP server and the actual transferring of files is encrypted. This ensures that user passwords and transmitted data are protected.

By using 128-bit SSL encrypted FTP, files are safely and securely transmitted and received over the Internet. All commands and data transmitted from one computer to the other are encrypted and can only be decrypted by the two parties involved in the data transfer.

The client software on your system must have the Secure FTP flag set to "ON" or you will not be able to log in to the HPES SFTP server.

When HPES receives your enrollment forms and establishes your service center code, we also assign you a username and password for the SFTP server (see heading, Passwords).

You must change your HPES SFTP server password at least every 30 days.

The following are the minimum requirements for accessing the HPES SFTP server:

- A valid username and password assigned to you from HPES
- Explicit 128-bit SSL Encryption
- Passive Mode
- Secure FTP flag must be set to on. When you have met the requirements above, you may log in to the HPES SFTP server using the following hostname and port:

☐ Hostname: Secureftp.fhsc.com

Remote (Control) Port: 21000

Service centers that reside behind a firewall must allow outbound sessions to be established on ports 21001-21100 for the datachannel of the FTP connection.

The Division of Health Care Financing and Policy (DHCFP) requires that service centers, intermediaries and software vendors provide proof of transaction testing and certification through Level II, as outlined by WEDI. This certification is a prerequisite for business-tobusiness testing with DHCFP. Certification can be through Claredi or another certifying entity.The DHCFP has certified its outbound transactions to Level 6 through Claredi.

Directory Setup

After establishing a connection to the HPES SFTP server, you will be able to see the following directories, which are described in the following sections:

- Incoming
- Outgoing
- Test
- Hold

Incoming

This is a directory used by a service center to electronically submit transaction sets for production. If your service center has not successfully tested with HPES, files you place in this directory will not be processed through the compliance checker and HPES will notify you that your file was rejected.

If your service center has successfully tested with HPES, we will process the file and the proper response will be placed in your outgoing directory. You may use your own file naming convention. HPES recommends that all files you place into this directory be zipped. All zipped files must have a .zip suffix inorder for us to process them. When HPES receives the file we rename it with a Media Control Number (MCN) and begin processing it. After you place files in this directory, it is not possible to delete them. If you place files ther by mistake, you must file an adjustment request or void after you receive your Remittance Advice (RA). A *.rpt (report) file will be placed into your outgoing directory advising you of the MCN.

Outgoing

This is directory used by HPES to place files ready for you to retrieve (e.g., 271, 277, 835 or 997 transactions). All files placed in this directory will be zipped and must be unzipped using PKUNZIP, WINUNZIP or a similar product.

It is imperative that you download files regularly and often. All files in this directory remain on the system for a period of 45 days. The HPES SFTP server automatically deletes files that have resided in this directory over 45 days. When you log in, you will be able to retrieve all files still in this directory.

Test

This directory is used to place test transaction sets. HPES tests files that you place in this directory to ensure there are no file errors.

Hold

This directory is used by HPES during the processing of files. Do not delete or download files from this directory. Do not place any files in this directory for processing.

Testing

Testing is critical to the electronic transaction process. The following sections apply to all service centers.

Pre-Test Requirements

After you submit the Service Center Operational Information Form (FA-36) and the Electronic Transaction Agreement for Service Centers (FA35), HPES assigns a service center code to the submitter and an account on the HPES SFTP server is established.

After you submit these forms, we will contact you with your SFTP username, your initial password and your service center code.

Your 837 test transmission should contain between 25 and 50 claims relevant to the provider's specialty. Other transactions have no low limits but should not exceed 50.

Test Requirements

All electronic transactions received by HPES after October 15, 2003 must be in the HIPAA compliant format. This format is currently ANSI X12N Version 4010A1.

SSL FTP File Transfer

After you receive your service center code from HPES, complete the following to enact the test transmission.

- Enter your test transmission. ☐
- Connect to the HPES SFTP server at secureftp.fhsc.com using your assigned username and password. In the event of difficulties contact the EDI Coordinator.

Once your test file is processed, we will place two files in your outgoing directory:

- The *.rpt file contains identification for the transaction also called a Media Control Number ("MCN").
- The 997 response notifies you that HPES has received your test transmission and whether it was accepted or rejected.

If you do not receive this response, call the EDI Coordinator at (877)638-3472.The 997 transaction notifies you that HPES has received your test transmission.

HPES then evaluates your test file. We will notify you by phone upon successful completion of the test.

In the event that the test transmission is unsuccessful, we will provide youw tih a report indentifying the transaction errors. Another test file is required.

Test Results Notification

HPES normally completes test transaction evaluation within two working days. If you do not receive a 997 transaction within two working days or an appropriate final response (271, 277, 835, etc.) within five working days, call the EDI Coordinator.

Successful Test Transaction

The EDI Coordinator will notify you by phone of a successful test transaction and inform you of the date that you may begin sending and retrieving transactions in production.

Unsuccessful Test Transaction

A list of errors is generated for each unsuccessful test transaction. HPES will mail or fax this list to you upon your request. Another test transaction must be completed before you may begin sending and receiving transactions in production.

Production Transactions

After HPES notifies you of a successful test, you may begin to send files to the SFTP server by placing them in your incoming directory for processing and retrieve processed files from your outgoing directory.

The HPES SFTP server is available to receive electronic submissions seven days a week, 24 hours a day.

Password Change

As part of the requirements for HIPAA security, you must change your SFTP server password every 30 days. Your password must be at least six characters in length and can not be the same as any of your last six passwords. It is important to note that no notice will be provided that your password will expire or has already expired. If it has already expired, you will not be able to log into the server.

The following process for changing your SFTP server password command may vary depending on the FTP client you are using. Please see your software documentation for additional information.

To change your password before it expires, do the following:

- Log in to the SFTP server
- Type the SITE command:
  - chgpsw
- Then type the following syntax all on one line:
  - username oldpassword newpassword newpassoword

For example, if your username is mike_smith, your old password is 123456 and you want to change your password to abcdef, you would type the following all on one line:

  - chgpsw mike_smith 123456 abcdef abcdef

Wait while the chgpsw command executes and the servers process the request. Once the process has been completed, you will receive one of the following messages:

Server Message	Explanation
Password successfully changed!	If you receive this message the process completed successfully and your password has been changed.
SERVERNAME/USERNAME: Password did not match	This error will occur if you do not specify your existing password properly. Please enter the command again with the correct password.
New passwords do not match- Error!	This message indicates that the new password specified was not re-typed correctly. Please try again.
Not enough arguments- Error!	Syntax – SITE chgpsw username oldpassword newpassword newpassword. One of the values needed was missing. Please verify that all of the required information is provided and try again.

Server Message	Explanation
New and old password must be different- Error!	New passwords are required to be different from your existing password or any of your last six passwords. Please choose a different new password and try again.

Other errors similar to the ones above may also be encountered. Most of them should be clear enough to identify what caused them but if there are any problems or concerns, please contact the EDI Coordinator.

If your password has already expired and you know what your password was, call the Help Desk at (804) 965-7782. They will reset the password so you will be able to log into the SFTP server. The HPES Help Desk hours are Monday through Friday from 6:00 a.m. until 8:00 p.m. ET except on holidays.

If your password has already expired and you do not remember your password, call the EDI Help Desk at (800) 638-3472 and select the option for electronic billing. The EDI Help Desk authenticates your service center and issues you a new password. The EDI Help Desk hours are Monday through Friday from 8:00 a.m. until 4:00 p.m. MT except on holidays.